UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/668,408	09/22/2000	Carl M. Ellison	042390.P8628X	2377

8791 7590 04/07/2004

BLAKELY SOKOLOFF TAYLOR & ZAFMAN
12400 WILSHIRE BOULEVARD, SEVENTH FLOOR
LOS ANGELES, CA 90025

EXAMINER	
ARANI, TAGHI T	

ART UNIT	PAPER NUMBER
2131	10

DATE MAILED: 04/07/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/668,408	ELLISON ET AL.	
	Examiner	Art Unit	
	Taghi T. Arani	2131	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE ____ MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *9/22/2000*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-60* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-60* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date *3-6,8-9*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

Claims 1-60 were pending for examination.

Claim Rejections - 35 USC § 112

The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

Claims 3-15, 18-30, 33-45, 48-60 rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

Claim 3 (lines 5 and 7), claim 18 (lines 3, 4 and 5), claim 33 (lines 3, 6 and 7), claim 48 (lines 3, 5 and 7) recites the limitation "the identifiers". There is insufficient antecedent basis for this limitation in the claim.

Dependent claims 4-15, 19-30, 34-45 and 49-60 are also rejected by virtue of their dependencies.

For the purpose of applying art, the Examiner assumes "cryptographic identifiers".

Double Patenting-35 U.S.C. 101

A rejection based on double patenting of the "same invention" type finds its support in the language of 35 U.S.C. 101 which states that "whoever invents or discovers any new and useful process ... may obtain a patent therefor ..." (Emphasis added). Thus, the term "same invention," in this context, means an invention drawn to identical subject matter. See *Miller v. Eagle Mfg. Co.*, 151 U.S. 186 (1894); *In re Ockert*, 245 F.2d 467, 114 USPQ 330 (CCPA 1957); and *In re Vogel*, 422 F.2d 438, 164 USPQ 619 (CCPA 1970).

A statutory type (35 U.S.C. 101) double patenting rejection can be overcome by canceling or amending the conflicting claims so they are no longer coextensive in scope. The filing of a terminal disclaimer cannot overcome a double patenting rejection based upon 35 U.S.C. 101.

Claims 1, 16, 31 and 46 are provisionally rejected under 35 U.S.C. 101 as claiming the same invention as that of claims1, 16, 31 and 46 of copending Application No. 09/540,613. This is a provisional double patenting rejection since the conflicting claims have not in fact been patented.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

Claims 1, 16, 31 and 46 are rejected under 35 U.S.C. 102(e) as being anticipated by Barnett, U.S. Patent No. 6,292,874, filed Oct. 1999.

As per claim 16, Barnett is directed to a memory management unit for a single-chip data processing circuit, such as a smart card, see abstract.

Barnett teaches that "The memory management unit(i) partitions a homogeneous memory device to achieve heterogeneous memory characteristics for various regions executing of the microprocessor core to predetermined memory ranges. Thus, the memory management unit imposes firewalls between applications and permits hardware checked partitioning of the memory. The memory management unit provides two operating modes for the processing circuit. In a secure kernel mode, the programmer can access all resources of the device including

hardware control. In an application mode, the memory management unit translates the virtual memory address used by the software creator into physical address allocated to the application by the operating system in a secure kernel mode during installation", see col. 2, lines 47-65.

Claims 1, 31 and 46 are apparatus, computer program product and system corresponding to method claim 1. Claims 1, 31 and 46 are rejected for the same reasons provides in the statement of rejection of claim 1 above.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claims 2, 17, 32, 47 are rejected under 35 U.S.C. 103(a) as being unpatentable over Barnett as applied to claims 1, 16, 31 and 46 above and further in view of Panwar et al., U.S. Patent No. 6,035,374, filed June 1997.

As per claim 17, Barnett teaches that "the memory management unit provides two operating modes for the processing circuit. In a secure kernel mode, the programmer can access all resources of the device including hardware control. In an application mode, the memory management unit translates the virtual memory address used by the software creator into the physical address allocated to the application by the operating system in a secure kernel mode during installation", see col. 2, lines 58-65. This clearly suggests "storing a chipset mode

indicating a mode of operation of the chipset in a mode storage; and writing the chipset mode into the mode storage".

Barnett is silent on "*storing a thread count in a thread count storage indicating number of threads currently operating in the isolated execution mode; updating the thread count when the initialization storage is accessed*".

However, Panwar teaches, in col. 13, lines 9-35, "ISU 206 (see Fig. 8) is operative to schedule and dispatch instructions as soon as their dependencies have been satisfied into an appropriate execution unit (FGU 210). ISU 206 also maintains trap status of live instructions. ISU 206 may perform other functions such as maintaining the correct architectural state of processor 102, including state maintenance when out-of-order instruction processing is used. ISU 206 may include mechanisms to redirect execution appropriately when traps or interrupts occur and to ensure efficient execution of multiple threads where multiple threaded operation is used. Multiple thread operation means that processor 102 is running multiple substantially independent processes simultaneously" and that "state machine 301 are implemented in ISU 206 by maintaining virtual processor status information in ISU 206. Although other functional units use the thread ID to implement multiprocessors in accordance with the present information, ISU 206 uses the virtual processor status information .....hence, to ease circuit complexity and improve operation speed, it is advantageous to implement state machines 301 in ISU 206".

It would have been obvious to one of ordinary skill in the art at the time of the invention to modify Barnett's method of initializing a chipset with multiprocessors with isolated and normal execution modes to include a method for counting processors being utilized. One of

ordinary skill in the art would have been motivated to perform such a modification because the method of executing coded instruction in a dynamically configurable multiprocessor is a well known in the art, see col. 4, lines 38-55 of Panwar.

Claims 2, 32 and 47 are apparatus, computer program product and system corresponding to method claim 17. Claims 2, 32 and 47 are rejected for the same reasons provides in the statement of rejection of claim 17 above.

Claims 3-14, 18-29, 33-44 and 48-59 are rejected under 35 U.S.C. 103(a) as being unpatentable over Barnet and Panwar as applied to claims 1-2, 16-17, 31-32, 46-47 above and further in view of Peinado et al, U.S. Pub. No. 2002/0007456, filed June 2001.

As per claims 18-19, Barnett and Panwar fail to teach "storing cryptographic identifiers of the executive operating in the isolated execution mode, the identifiers being read only when in lock; storing a lock pattern indicating the identifiers in lock; and locking the identifiers based on the lock pattern" and claim 19 " and " storing a platform key used in handling the executive entities in platform key storage and storing isolated settings used to configure the isolated execution mode".

However, Peinado teaches " In the present invention, the secure processor 64 is constructed to include a security (CPU) key 66 physically hard-wired (permanently stored) thereinto, and the security kernel 68 is also physically hard-wired thereinto, where only the security kernel 68 can access the CPU key 66..... . the secure processor 64 is operable in a normal mode and a preferred mode, where the security kernel 68 can access the CPU key 66 only

during the preferred mode....., the accessed CPU key 66 is employed by the security kernel 68 to decrypt one or more encrypted security keys for the application 72 instantiated....., the security kernel 68 ensures that each application 72 has access to the secrets of such application 72, and does not have access to the secrets of any other application 72. As a result, each application 72 on the portable device 62 is isolated from every other application 72 on the portable device 62. Such functionality is required for banking applications (credit card numbers, PINs, e.g.) and DRM applications (private keys, e.g.)....., the accessed CPU key 66 and/or the decrypted key(s) may be employed by the security kernel 68 to authenticate/verify the application 72 to be instantiated. In particular, the application 72 may include a certificate or the like, and the security kernel 72 may perform a hash or MAC (message authentication code) over the code for the application based on the CPU key 66 and then compare the hash or MAC to the certificate or the like", page 21,paragraphs 290-294.

It would have been obvious to one of ordinary skill in the art at the time of invention to modify the method of initializing a chipset with multiprocessor with isolated and normal execution modes and counting the status of the processors taught in the combination of Barnet and Panwar key mapped to the isolated location. One of ordinary skill in the art would have been motivated to perform such modification because security keys (and authentication through certificate) with enforcement architecture are often used when managing digital rights, see Peinado, page 1 paragraphs 10-11.

As per claim 20, Panwar teaches "A processor in accordance with the present invention includes a processor creation unit responsive to a processor create command to output signals indicating a current processor configuration and plurality of virtual or logical processors each virtual processor having a first set of execution resources that are uniquely identified with the virtual processor and a second set of execution resources that are shared amongst the plurality of virtual processors", see col. 4, lines 38-48.

As per claim 21, Panwar teaches that " A plurality of state machines responsive to the processor creation unit are provided, each corresponding to a selected one of the plurality of virtual processors. The state machines maintain processor status information representative of whether the processor is available to receive and execute instructions".

As per claim 22, Panwar teaches that "Once a branch is resolved, the address of the path this branch actually follows is communicated from IEU 208 and compared against the predicted path address store in the BT ADDRESS fields. If these two addresses differ, those instructions down the mispredicted path are flushed from the processor and IFU 202 redirects instruction fetch down the correct path identified in the BNT ADDRESS field using the BRT input to MUX 505. Once a branch is resolved, the BHT value is updated using the BHT index and BHT value stored in BRT 515. In the example of FIG. 5, each entry in BHT 519 is a two-bit saturating counter. When a predicted branch is resolved taken, the entry used to predict this outcome is incremented. When a predicted branch is resolved not taken, the entry in BHT 519 is decremented. Other branch prediction algorithms and techniques may be used in accordance with

the present invention, so long as care is taken to duplicate resources on a processor-by-processor basis where those resources are used exclusively by a given processor", col. 10, lines 18-36.

As per claims 23, Panwar discloses that " ISU 206 (shown in greater detail in FIG. 8) is operative to schedule and dispatch instructions as soon as their dependencies have been satisfied into an appropriate execution unit (e.g., integer execution unit (IEU) 208, or floating point and graphics unit (FGU) 210). ISU 206 also maintains trap status of live instructions, col. 13, lines 9-15.

As per claim 24, Panwar teaches that "The processor further includes status logic analyzing expected latency of instructions on each processor and updating the state machine corresponding to any processor having an instruction with an expected latency greater than a preselected threshold", see col. 4, lines 51-5.

As per claim 25, Panwar teaches "IFU 202 includes instruction marker circuitry 507 for analyzing the fetched instructions to determine selected information about the instructions. Marker unit 507 is also coupled to processor create unit 200. This selected information, including the thread identification (i.e., the virtual processor identification) generated by processor create unit 200, is referred to herein as "instruction metadata". In accordance with the present invention, each fetch bundle is tagged with a thread identification for use by downstream functional units. Other metadata comprises information about, for example, instruction complexity and downstream resources that are required to execute the instruction. The term "execution resources" refers to architectural register space, rename register space, table space, decoding

stage resources, and the like that must be committed within processor 102 to execute the instruction, col. 11, lines 3-19.

As per claim 26, Panwar teaches "Once a branch is resolved, the address of the path this branch actually follows is communicated from IEU 208 and compared against the predicted path address store in the BT ADDRESS fields. If these two addresses differ, those instructions down the mispredicted path are flushed from the processor", col. 10, lines 18-23.

As per claim 27, Peinado teaches "the root entity returns the license server public key (PU-LS) to such license server 24 encrypted with the private root key (PR-R) (i.e., (CERT (PU-LS) S (PR-R)))", page 15, paragraph 220.

As per claim 28, Peinado teaches that " the secure processor 64 is constructed to include a security (CPU) key 66 physically hard-wired (permanently stored) thereinto, and the security kernel 68 is also physically hard-wired thereinto, where only the security kernel 68 can access the CPU key 66. Such physical hard-wiring may be performed during manufacturing of the secure processor 64 and may be done in any appropriate manner without departing from the spirit and scope of the present invention. Such physical hardwiring is known or should be apparent to the relevant public and therefore need not be described herein in any detail. For example, the secure processor 64 may be manufactured with storage space 70 for a CPU key 66 and a security kernel 68, where the storage space 70 is in the form of ROM to be pre-programmed by the manufacturer", page 21, paragraph 290.

As per claim 29, Peinado teaches that "Once the downloaded license has been stored in the DRM system license store, the user can render the digital content according to the rights conferred by the license and specified in the license terms. When a request is made to render the digital content, the black box is caused to decrypt the decryption key and license terms, and a DRM system license evaluator evaluates such license terms. The black box decrypts the encrypted digital content only if the license evaluation results in a decision that the requester is allowed to play such content. The decrypted content is provided to the rendering application for rendering.

In the present invention, a secure processor for a computing device is operable in a normal mode and a preferred mode, and includes a security kernel for being instantiated on the processor when the processor enters into the preferred mode and a security key accessible by the instantiated security kernel when the processor is operating in the preferred mode. The security kernel employs the accessed security key during the preferred mode to authenticate a secure application on the computing device, and allows the processor to be trusted to keep hidden a secret of the application", page 2, paragraphs 17-18.

Claims 3-14, 33-44 and 48-59 are apparatus, computer program product and system corresponding to method claims 18-29. Claims **3-14, 33-44 and 48-59** are rejected for the same reasons provides in the statement of rejections of claims 18-29 above.

Claims 15, 30, 45 and 60 are rejected under 35 U.S.C. 103(a) as being unpatentable over Barnett, Panwar and Peinado as applied to claims 4, 19, 34 and 49 above and further in view of Ellison et al., U.S. Patent No. 6,507,904, filed March 2000.

As per claim 30, Barnett, Panwar and Peinado fail to teach "*wherein the isolated settings include an isolated base value, an isolated length value, and a processor executive entry address, the isolated base and length values defining the isolated memory area.*".

However, Ellison teaches "The system of claim 29 wherein the at least one parameter is one of an isolated feature word, an execution mode word, a logical processor value, an isolated setting including a mask value and a base value, a frame, an exit physical address, an entry physical address, and a processor nub loader physical address" in claim 30, col. 16, lines 62-67.

It would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the method of initializing a chipset with multiprocessors with isolated and normal execution modes, counting the status of the processors and utilizing a key taught in the combination of Barnett, Panwar and Peinado to include masked values (i.e. length value). One of ordinary skill in the art would have been motivated to perform such a modification because mask values (length values) are used with isolated processors and "One principle for providing security in a computer system or platform is the concept of an isolated execution architecture. The isolated execution architecture includes logical and physical definitions of hardware and software components that interact directly or indirectly with an operating system of the computer system or platform. An operating system and the processor

may have several levels of hierarchy, referred to as rings, corresponding to various operational modes.", col.3, line 59-67 stating (Ellison).

Claims 15,45 and 60 are apparatus, computer program product and system corresponding to method claim 30. Claims **15, 45 and 60** are rejected for the same reasons provides in the statement of rejections of claim 30 above.

Conclusion

Any inquiry concerning this communication or earlier communications from examiner should be directed to Taghi Arani, whose telephone number is (703) 305-4274. The examiner can normally be reached Monday through Friday from 8:00 AM to 5:30 PM.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh, can be reached at (703) 305-9648. The Fax numbers for the organization where this application is assigned is:

(703) 872-9306

Taghi Arani

Patent Examiner

3/31/2004

AYAZ SHEIKH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100